Security Level of Cryptography- PSEC

1 Cryptographic Primitive

Name: PSEC

Category: Asymmetric Cryptographic Schemes

Security Function: Confidentiality

2 Evaluation

2.1 The Underlying Number Theoretic Problem

The scheme is based on the Diffie-Hellman problem over EC. It can be viewed as augmenting the SEC– ECAES proposal with mechanics analogous to the EPOC one. Namely, the random oracle preprocessing (which I suggested to be used uniformly anyway in any scheme used).

The scheme is actually three schemes,

PSEC-1,-2 and -3.

Some of the schemes are directed towards the hybrid encryption mode.

The underlying number theoretic structure is an Elliptic Curve over a prime order field.

2.2 Semantic security evaluation

Under the assumptions mentioned by the authors (e.g., Decisional D-H ECC), the schemes are semantically secure (against passive adversary).

2.3 Complexity Theory and Security against active attacks

The scheme employs auxiliary functions like hash function (idealized as random oracle) for the preprocessing (the Okamoto Pointcheval preprocessing of messages). Assuming the random oracle, preprocessing the schemes are proven secure against the strongest attack (adaptive chosen attack). The proofs are not given in full details, yet they seems plausible by analogy to the existing proofs.

The envelope (hybrid) method is given, which makes sense with the EC method. As mentioned in reviewing SEC a method to have a mode of encryption concatenating related messages is suggested.

2.4 Other problems, issues and considerations

It is suggested the complete proof will be done for this suggestion, though the analogy from D-H/ ElGamal is understood. The paper justifying the method is now only an extended abstract. I drew analogies and verified the proof as much as possible, but the provable security has to be better explained in proofs.

CLOSET ALTERNATIVES AND COMPARISON: If one performs ECC, the added value of preprocessing is obvious, it does not cost much and one claim validate security to chosen ciphertext attacks (in the random oracle model).

Cramer-Shoup EC alternative may be used, it has the obvious advantage of not needing random oracle to claim CCA security. It is slower though(half the speed and even less).